IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION

PACSEC3, LLC,	)	
Plaintiff,	)	
	)	**Civil Action No. 6:20-CV-00914-ADA**
v.	)	
	)	
NETSCOUT SYSTEMS, INC.,	)	**JURY TRIAL DEMANDED**
Defendant.	)	

PLAINTIFF'S OPENING CLAIM CONSTRUCTION BRIEF

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

I. INTRODUCTION

Plaintiff PacSec3, LLC ("PacSec") asserts US 6,789,190 ("the '190 patent") (Claim 1); US 7,047,564 ("the '564 patent") (Claims 1-6); and, US 7,523,497 ("the '497 patent") (Claims 1, 4, 7, 10, 13, 16) (collectively, the "Asserted Patents") against NetScout, Inc. ("NetScout")'s Distributed Denial of Service ("DDoS") attack protection products including Peakflow SP/Peakflow SP TMS (and other Peakflow versions).

II. BACKGROUND

A. Patents

1. The '190 Patent

Embodiments of the '190 patent relate to systems and methods for preventing "packet flooding" or DDoS attacks where an attacker uses up all available bandwidth with a victim, typically supplying useless data and to prevent other related denial of service attacks. The defense is distributed among cooperating sites and routers. [1] The claimed invention solved prior art problems associated with association of data packets for which bandwidth should be fairly allocated and control over which packets are allowed to arrive.[2] In essence, the '190 patent claims a technical solution to these problems through cooperating sites and routers.[3] PacSec3 is asserting Claim 1 of the '190 patent.

2. The '564 patent

Embodiments of the '564 patent relate to systems and methods to reduce or limit DDoS attacks by identifying and classifying data packets arriving at a "Reverse Firewall" for

[1] *See* Doc. No. 1-1, '190 patent at Abstract.
[2] *See* Doc. No. 1-1, '190 patent at Column 1, line 65 to Column 2, line 4 ("1:65-2:4").
[3] *See* Doc. No. 1-1, '190 patent at 2:5-16.

transmission to the external network.[4] The '564 patent claims a technical solution comprising a firewall that includes hardware and software providing a non-redundant connection between networks and serves to control packet transmission between the networks.[5] PacSec3 is asserting Claims 1-6 of the '564 patent.

3. The '497 patent

Embodiments of the '497 patent relate to systems and methods to reduce or limit DDoS attacks by identifying and classifying data packets arriving at a cooperating router for transmission to the external network.[6] The '497 patent claims a technical solution comprising a host computer, router, communication lines and transmitted data packets.[7] PacSec3 is asserting Claims 1, 4, 7, 10, 13, and 16 of the '497 patent.

B. The Accused NetScout Systems

PacSec3 accuses NetScout of directly infringing the Asserted Patents through Defendant's Arbor DDoS system.[8]

II. LEGAL PRINCIPLES

a. General Claim Construction Principles

Determining the proper meaning of patent claims is a question of law that exclusively belongs to the Court.[9] During claim construction, a court first looks at the words of the claims

[4] *See* Doc. No. 1-2, '564 patent at Abstract.
[5] *See* Doc. No. 1-2, '564 patent at 3:32-42.
[6] *See* Doc. No. 1-3, '497 patent at Abstract.
[7] *See* Doc. No. 1-3, '497 patent at 3:30-42.
[8] https://www.netscout.com/arbor-ddos#section--1.
[9] *Markman v. Westview Instruments, Inc.*, 52 F.3d 967, 970-71 (Fed. Cir. 1995) (en banc), *aff'd*, 517 U.S. 370 (1996).

themselves to define the scope of the patented invention.[10] In determining the meaning of the claims, "there is a 'heavy presumption in favor of the ordinary meaning of claim language.'"[11] Ordinary meaning is defined as the "meaning that term would haveto a person of ordinary skill in the art in question at the time of invention."[12]

b. Requirements under 35 U.S.C. §112(f).

The use of the term "means" triggers a rebuttable presumption that *§ 112*, ¶ 6 [now *§ 112(f)*] applies.[13] The presumption that 35 USC 112(f) applies is overcome when the limitation further includes the structure, material or acts necessary to perform the recited function. "Sufficient structure exists when the claim language specifies the exact structure that performs the function in question without need to resort to other portions of the specification or extrinsic evidence for an adequate understanding of the structure."[14] The standard is whether the words of the claim are understood by persons of ordinary skill in the art (POSITA) to have a sufficiently definite meaning as the name for structure.[15]

Another manner in which this presumption can be overcome is if "the claim recites sufficient structure for performing the described functions in their entirety."[16] To determine if the

[10] *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312 (Fed. Cir. 2005) (en banc).
[11] *Watts v. XLSys., L.P.*, No. 1:06-cv-653-LY, 2008 WL 5731945, at *7 (W.D. Tex. July 1, 2008) (quoting *Johnson Worldwide Assocs. v. Zebco Corp.*, 175 F.3d 985, 989 (Fed. Cir. 1999)); *see also MeetrixIP, LLC v. Citrix Sys., Inc.*, No. 1:16-CV-1033-LY, 2017 WL 5986191, at *2 (W.D. Tex. Dec. 1, 2017) (citing *Thorner v. Sony Computer Entm't Am. LLC*, 669 F.3d 1362, 1365 (Fed. Cir. 2012))("The Federal Circuit has reaffirmed that a departure from the ordinary and customary meaning isthe exception, not the rule.").
[12] *Phillips*, 415 F.3d at 1313; *see also Pisony v. Commando Construction, Inc.*, W-17-CV-00055-ADA, 2019 WL 928406,at *1 (W.D. Tex. Jan. 23, 2019). "[T]he person of ordinary skill in the art is deemed to read the claim term not only in the context of the particular claim in which the disputed term appears, but in the context of the entire patent, including the specification." *Phillips*, 415 F.3d at 1313.
[13] *TecSec, Inc. v. IBM*, 731 F.3d 1336, 1348-9 (Fed. Cir. 2013) *citing TriMed, Inc. v. Stryker Corp., 514 F.3d 1256, 1259 (Fed. Cir. 2008)*.
[14] See *TriMed, Inc. v. Stryker Corp.,* 514 F.3d 1256, 1259-60, 85 USPQ2d 1787, 1789 (Fed. Cir. 2008); ; see also *Altiris, Inc. v. Symantec Corp.,* 318 F.3d 1363, 1376, 65 USPQ2d 1865, 1874 (Fed. Cir. 2003).
[15] *Williamson v. Citrix Online, LLC,* 792 F.3d 1339, 1349 (Fed. Cir. 2015).
[16] *Id.*

claim recites sufficient structure, "it is sufficient if the claim term is used in common parlance or by persons of skill in the pertinent art to designate structure, even if the term covers a broad class of structures and even if the term identifies the structures by their function."[17]

If persons of ordinary skill in the art reading the specification understand the term to have a sufficiently definite meaning as the name for the structure that performs the function, even when the term covers a broad class of structures or identifies the structures by their function (e.g., "filters," "brakes," "clamp," "screwdriver," and "locks") 35 USC 112(f) will not apply.[18] Many devices take their names from the functions they perform. The term is not required to denote a specific structure or a precise physical structure to avoid the application of 35 USC 112(f).[19] The following are examples of structural terms that have been found **not** to invoke 35 USC 112(f): "circuit," "detent mechanism," "digital detector," "reciprocating member," "connector assembly," "perforation," "sealingly connected joints," and "eyeglass hanger member." Likewise, the Federal Circuit found the recitation of "aesthetic correction circuitry" sufficient to avoid a means plus function analysis or treatment because the term "circuit," combined with a description of the function of the circuit, connoted sufficient structure to one of ordinary skill in the art.[20]

For claims employing a computer implemented means-plus-function limitation where sufficient structure is determined not to have been disclosed, to avoid indefiniteness, the specification must disclose a special purpose computer as corresponding structure—*i.e.*, a

[17] *Williamson v. Citrix Online, LLC,* 792 F.3d at 1349*, citing Lighting World, Inc. v. Birchwood Lighting, Inc., 382 F.3d 1354, 1359-60 (Fed. Cir. 2004)*.
[18] *Apex Inc. v. Raritan Computer, Inc.,* 325 F.3d 1364, 1372-73, 66 USPQ2d 1444, 1451-52 (Fed. Cir. 2003)
[19] *Greenberg v. Ethicon Endo-Surgery, Inc.,* 91 F.3d 1580, 1583, 39 USPQ2d 1783, 1786 (Fed. Cir. 1996) ("See *Watts,* 232 F.3d at 880, 56 USPQ2d at 1838; *Inventio AG v. Thyssenkrupp Elevator Americas Corp.,* 649 F.3d 1350, 99 USPQ2d 1112 (Fed. Cir. 2011) (holding that the claim terms "modernizing device" and "computing unit" when read in light of the specification connoted sufficient, definite structure to one of skill in the art to preclude application of 35 [USC112(f)]).
[20] *Mass. Inst. of Tech. v. Abacus Software*, 462 F.3d 1344, 1359-1360 (Fed. Cir. 2006).

computer programmed to perform a disclosed algorithm.[21] An algorithm may be disclosed in "any understandable terms including as a mathematical formula, in prose, or as a flow chart, or in any other manner that provides sufficient structure."[22] However, "[s]imply reciting 'software' without providing some detail about the means to accomplish the function is not enough."[23] The party alleging that the specification fails to disclose sufficient corresponding structure must make that showing by clear and convincing evidence.[24]

c. Level of Ordinary Skill in the Art

From my review of the Patents-in-Suit, taking into account my education and experience, I am of the opinion that a person of ordinary skill in the art ("POSITA") at the time of the filing of the Asserted Patents or Patents-in-Suit would have at least a Master of Science ("MS") Degree in Computer Science or Computer Engineering, or equivalent work experience in the field of computer networks, along with knowledge of the general structure of networked communication systems, its hardware and software components and underlying communications technologies. In addition, a POSITA would be familiar with the latest communications standards.[25]

III. DISPUTED CLAIM TERMS

1. means for classifying data packets received at said firewall[26]

Plaintiff's proposed construction	Defendant's proposed construction	By:[27]
Function: identifying classes of the data packets that are received at said firewall	Indefinite	J

[21] *Ergo Licensing, LLC v. CareFusion 303, Inc*., 673 F.3d 1361, 1364-65 (Fed. Cir. 2012).
[22] *Finisar Corp. v. DirecTV Grp., Inc*., 523 F.3d 1323, 1340 (Fed. Cir. 2008) (internal citation omitted).
[23] *TecSec, Inc.*, 731 F.3d at 1348-9.
[24] *Id.*, *citing Budde v. Harley-Davidson, Inc*., 250 F.3d 1369, 1380-81 (Fed. Cir. 2001).
[25] See Declaration of Krishnamurthy Narayanaswamy, Ph.D. ("Narayanaswamy Decl.") at ¶13.
[26] Claim 1 of the '190 patent; Claim 1 of the '564 patent.
[27] J=Joint; P=Plaintiff; D=Defendant

Structure: 1:57 to 2:4; 3:1 to 3:5; Fig 1: 4:54 to 4:59 and 5:37 to 5:51; Fig 4: 5:3 to 5:6 and 6:13 to 6:24; Fig 7: 5:18 to 5:22 and 6:55 to 7:3		

2. means for associating a maximum acceptable transmission rate with each class of data packet received at said firewall[28]

Plaintiff's proposed construction	**Defendant's proposed construction**	**By:**
Function: associating a maximum threshold rate of transmission for each identified packet class through said firewall Structure: 1:65 to 2:4; 3:6 to 3:12; Fig 1: 4:59 to 4:54 and 5:37 to 5:51; Fig 4: 5:3 to 5:6 and 6:13 to 6:24; Fig 7: 5:18 to 5:22 and 6:55 to 7:3	Indefinite	J

3. means for said firewall to find information for packets it receives regarding the path by which said packets came to Said firewall[29]

Plaintiff's proposed construction	**Defendant's proposed construction**	**By:**
Function: providing the firewall with the path through which the packets were forwarded to the firewall Structure: 2:4 to 2:17; 3:6 to 3:12; 4:14 to 4:18; Fig 1: 4:59 to 4:54 and 5:37 to 5:51; Fig 4: 5:3 to 5:6 and 6:13 to 6:24; Fig 7: 5:18 to 5:22 and 6:55 to 7:3	Indefinite	J

Plaintiff groups these three terms together as the disclosure of structure and argument is largely coextensive. However, while Plaintiff contends these terms do not require the 112(f) analysis, Plaintiff's identified function and structure are provided in the boxed chart with argument and explanation following.

These claim terms are not subject to the requirements of 112(f) because from the perspective of one of ordinary skill in the art, the preamble of claim 1 of the '190 patent, followed by the subsequent claim language provide the structure of a router or firewall for each of "means for classifying...", means for associating..." and "means for said firewall..."[30] Both a router and

[28] Claim 1 of the '190 patent; Claim 1 of the '564 patent.
[29] Claim 1 of the '190 patent.
[30] See Narayanaswamy Decl. at ¶15.

a firewall have a very well-defined meaning in the art. A firewall is a device which is placed between two networks by the owner of one of those networks to safeguard that network from various network attacks.[31] These capabilities include identifying sets of data packets by certain properties (referred to as classification) and allocating a transmission rate to those packets identified by class. In the current invention, this method is extended to include information about the path taken by the packets as they traverse the computer network before they arrive at the firewall. A router is a device which forwards data packets to locations within a computer network. The data packets are forwarded along communication lines or paths between the appropriate parts of the computer network. It is very common for a router and/or a firewall to be part of securing a computer network for inspecting the contents of packets, and/or limiting the rates of transmission of specific sets of packets identified by properties (i.e., classification) including blocking that set of packets entirely.

One of ordinary skill in the art would understand that a router and a firewall provides the following capabilities:

1. classifying data packets received at the firewall;

2. associating a maximum acceptable transmission rate with each class of data packet received at said firewall; and,

3. receiving data packets from a path by which said packets came to the firewall.[32]

Plaintiff's proposed claim construction is further based on the literal language of the claim and the specification. First, the claim sets forth in the preamble that a packet flooding defense system of the invention includes a router.[33] Second, the "at least one firewall" comprises "hardware and software serving to control packet transmission" which one of ordinary skill in the art would know is a firewall that can be configured by software to provide the capabilities described.[34] This is sufficient structure for each of "means for classifying...", means for

[31] *See* Narayanaswamy Decl. at ¶15.
[32] *See* id. at ¶15.
[33] *See* Doc. No. 1-1 at 7:40-44.
[34] *See* id. at 7:45-47.

associating...” and “means for said firewall...”

In an alternative, adequate disclosure of the structure of a firewall and router is also disclosed in the specification. The claimed invention describes how the forwarding path for each packet is associated with that packet, thereby making it possible for a receiving computer to know that information. The software, or configuration, at the firewall is explained through the algorithms disclosed in Figure 1 by flowchart and diagram where a Class A and Class B (38) of a maximum acceptable processing rate (34) are assigned by the firewall to each data packet (30). The description provides that the computer can use the information, the maximum acceptable processing rate, to allocate the processing rate for each class (38) in a desired way among the places from which packets (30) are transmitted.[35] Figure 2, Figure 3, Figure 4, Figure 5, and Figure 6 illustrate additional embodiments, or algorithms, in which path information associated with each packet can be combined with other properties to classify the packet and assign it a transmission rate. Figure 7, Figure 8 and Figure 9 illustrate how a firewall protecting a network communicates the rate limit for packets routed to it or routed to it by class functions. Moreover, the marking of data packets by a firewall or router is within the ordinary parlance of one of ordinary skill in the art and as is disclosed in the highly related ‘497 patent.[36] Prior art discussed in the specification of the ‘190 patent (US5455865 and US6044402 for example) rely on the well-understood and accepted functionality of routers to maintain flow information between source and destination addresses by marking.[37] Marking of data packets that traverse a router is well-known in the art. Marking of data packets to encode path information is unique to this invention, and anyone familiar with firewalls would understand how to use a firewall capability to encode paths. The specification describes how a firewall and a router can add to packet information about the interface points where the packet entered the firewall or router.

The ‘190 patent provides very detailed description of packet marking. At 2:5-17, the ‘190

---

[36] *See* Doc. No. 1-3 at 3:64-66 (“which is done via packet marks provided by router....); *See* Narayanaswamy Decl. at ¶17.
[37] *See* Narayanaswamy Decl. at ¶17.

patent provided that the claimed invention provides a distributed defense:

> among cooperating sites and routers. A set of transitively connected cooperating machines is called a "cooperating neighborhood". The quality of the defense is related to the size of the cooperating neighborhood, a larger neighborhood providing better defense. Within the neighborhood it is possible to trace the forwarding path of packets. The association of packets with the "users" is approximated by associating packets with "places" in the cooperating neighborhood from which those packets are forwarded. That is, service will be allocated in a fair (or otherwise reasonable) manner among these places. A "place" in this sense is typically a particular interface from which a packet arrived at a cooperating router.

At 2:28-35, the '190 patent provides:

> Routers will supply data about the forwarding path of the packets that arrive at a site. The site can use this data to allocate service as described above among the packets that arrive. This would solve the problem of unfair service if the packets that arrived were a fair sample of those that were sent to the site. This may not be the case, however, if routers are unable to forward all the packets they receive.

At 2:38-43, the '190 patent provides:

> However another potential cause for this problem is a flooding attack against a router. That problem is solved by letting routers allocate their services in a similar way to that described above for sites. That is, they allocate the limited resource of forwarding bandwidth along any given output in a reasonable way among some set of places in the cooperating neighborhood

At 2:44-50, the '190 patent provides:

> The final step in the defense is that cooperating routers will limit the rate at which they forward packets to places that so request. This may not be essential in the allocation of service, but it is useful for limiting the bandwidth used by "unwanted" packets. The rate-limiting request is to be made when a site detects a high rate of unwanted packets coming from one place.

Figures 1, 2, 3, 4, 5, 6, 7 and 8 each illustrate illustrative methods of determining, by packet marking, how the path a packet takes is identified. These Figures, in cooperation with the written description, further provide various algorithms, by flowchart, used by the claimed invention to perform the claimed functions.[38]

[38] *See* Narayanaswamy Decl. at ¶19.

It is common parlance for one of ordinary skill in the art to use a router for

1. using a router or a firewall to mark data packets;[39]
2. associating a maximum acceptable transmission rate with each class of data packet;[40] and,
3. receiving data packets along identifiable paths;[41]

Prior art cited in this patent specification including US5455865 and US5353353 use such capabilities to implement other network attack defenses. In this patent specification the same capabilities are utilized to specify path information. The 190 patent's specification describes how a router can use the path information to limit the rate of transmission of packets with that path (i.e., that class of packet).[42]

4. whereby, said firewall can use said information to allocate the transmission rate for each class in a desired way[43]

Plaintiff's proposed construction	Defendant's proposed construction	By:
No construction necessary or "whereby, the firewall is capable of using the information to allocate the transmission rate for each class in a desired way"	whereby, said firewall uses said information to allocate thetransmission rate for each class in a desired way	D

Construction of long claim terms is disfavored.[44] Additionally, this "whereby" clause does not provide a limitation on the claim and need not be construed.[45] "A whereby clause in a method

[39] *See* Narayanaswamy Decl. at ¶21.
[40] *See* id. at ¶23.
[41] *See* id. at ¶25.
[42] *See* id. at ¶s 21, 23, 25.
[43] Claim 1 of the '190 patent.
[44] *Ihance, Inc. v. Eloqua Ltd.*, Civ. Act. No. 2:11cv2572012, U.S. Dist. LEXIS 62514, at *15, *16 (E.D. Va. May 2, 2012) (describing a 42-word term as "lengthy" and declining to construe the term); *Honeywell Int'l, Inc. v. Nikon Corp.*, 589 F. Supp. 2d 433, 440–444 (D. Del. 2008) (describing a 24-word term as "rather lengthy," then focusing on 2 words of the claim term, and ultimately declining to construe the 24-word term).
[45] *Tex. Instruments Inc. v. U.S. Int'l Trade Comm'n*, 988 F.2d 1165, 1172 (Fed.Cir.1993) (concluding, in process claims, that the whereby clauses described "the result of arranging the components of the claims in the manner recited in the claims" and thus were not limitations).

claim is not given weight when it simply expresses the intended result of a process step positively recited."[46] Thus, if a whereby clause adds nothing to the claims and simply characterizes the intended result of the executing steps, it need not be construed by the court.[47] Here, no meaningful limitation is added by this "whereby" clause and no construction is necessary.

5. path[48]

Plaintiff's proposed construction	Defendant's proposed construction	By:
Plain and ordinary meaning	each router	D

Path is a well-understood word.[49] There is nothing ambiguous about it and there is no evidence that the patent applicant clearly redefined (in the application or prosecution history). Thus, it should simply be construed as "plain and ordinary meaning."[50] Rejection of Defendant's proposed construction and adoption of a "plain and ordinary meaning" construction resolves the claim-construction dispute without need for further construction of the term.[51]

The defendant's proposed construction would render limitations in the claims of the '497 patent superfluous as Claim 1 of the '497 patent adds a limitation of "all routers." Defendant's construction would make the term "said each router comprising all routers." Further, a path and a router are separate terms and should not be construed as one term.

6. router[52]

Plaintiff's proposed construction	Defendant's proposed construction	By:
Plain and ordinary meaning	a device that determines the optimal path	D

[46] *Minton v. Nat'l Ass'n of Sec. Dealers, Inc.*, 336 F.3d 1373, 1381 (Fed. Cir. 2003) (*citing Tex. Instruments Inc.,* 988 F.2d at 1172).
[47] *See Minton*, 336 F.3d at 1381.
[48] 'Claim 1 of the '190 patent.
[49] *See* Narayanaswamy Decl. at ¶73.
[50] *See Arthrex*, 2016 U.S. Dist. LEXIS 105750, at **106, 108, 127 173, 174 (Payne, Mag).
[51] *PerdiemCo, LLC v. IndusTrack LLC*, No. 2:15-cv-727-JRG-RSP, 2016 U.S. Dist. LEXIS 87927, *64 (E.D. Tex. July 7, 2016 (stating, "The Court therefore expressly rejects Defendants' indefiniteness arguments. No further construction is necessary. [Citations and paragraph break omitted].
[52] Claim 1 of the '190 patent; Claims 1, 4, 7, 10, 13, and 16 of the '497 patent.

	along which communications traffic should be forwarded and that is not a firewall	

Router is a well-understood word.[53] There is nothing ambiguous about it and there is no evidence that the patent applicant clearly redefined (in the application or prosecution history) "router," an unambiguous term, it should simply be construed as "plain and ordinary meaning."[54]

7. host computer[55]

Plaintiff's proposed construction	Defendant's proposed construction	By:
Plain and ordinary meaning	a computer that processes received and transmitted data throughthe application layer and that is not a firewall	D

A Host Computer is a well-understood term.[56] There is nothing ambiguous about it and there is no evidence that the patent applicant clearly redefined (in the application or prosecution history) "host computer," an unambiguous term, it should simply be construed as "plain and ordinary meaning."[57]

8. means for limiting the transmission rate from the firewall to the maximum acceptable transmission rate for each class of data packet[58]

Plaintiff's proposed construction	Defendant's proposed construction	By:
Function: limiting the transmission rate from the firewall to the maximum acceptable transmission rate for each class of data packet Structure: 3:18 to 3:20; 3:42 to 3:49; 4:46 to 4:50; 5:10 to 5:18; Figure 1 provides details	Indefinite	J

[53] *See* Narayanaswamy Decl. at ¶74.
[54] *See Arthrex*, 2016 U.S. Dist. LEXIS 105750, at **106, 108, 127 173, 174 (Payne, Mag.).
[55] Claim 1 of the '190 patent; Claim 1 of the '564 patent; Claims 1, 4, 7, 10, 13, and 16 of the '497 patent.
[56] *See* Narayanaswamy Decl. at ¶76.
[57] *See Arthrex*, 2016 U.S. Dist. LEXIS 105750, at **106, 108, 127 173, 174 (Payne, Mag.).
[58] Claim 1 of the '564 patent.

The '564 patent discloses and claims a reverse firewall packet control system for controlling packet transmission between two networks.[59] From the perspective of one of ordinary skill in the art, the preamble of claim 1 of the '564 patent, [60] followed by the subsequent claim language provide the structure of a firewall comprising hardware and software for each of "means for classifying...", means for associating..." and "means for limiting the transmission rate..." A firewall has a very well-defined meaning in the art and is a device which controls the transmission of data between one or more networks. The data packets are forwarded along communication lines or locations between appropriate parts of the one or more networks. It is very common for a firewall to be between two networks, such as an internal network and an external network.[61]

One of ordinary skill in the art would understand that it is a firewall between two networks that is:

1. classifying data packets received at the firewall;

2. associating a maximum acceptable transmission rate with each class of data packet received at said firewall; and,

3. limiting the transmission rate from the firewall to the maximum acceptable transmission rate for each class of data packet.[62]

The literal language of the claim and the specification support this construction. First, the claim sets forth a firewall as the first element.[63] Second, the "at least one firewall" comprises "hardware and software ... serving to control packet transmission"[64] which one of ordinary skill in the art would know is a firewall with software, as a firewall controls packet transmission. Thus, sufficient structure is provided in the claim that each of "means for classifying...", "means for

[59] *See* Doc. No. 1-2 at 3:31-42; Narayanaswamy Decl. at ¶26.
[60] *See* Doc. No. 1-2 at 6:26-47.
[61] *See* Narayanaswamy Decl. at ¶26.
[62] *See* id.
[63] *See* Doc. No. 1-2 at 6:31-34.
[64] *See* id.

associating...” and “means for limiting...” are not properly considered as means plus function claim terms.

As an alternate position, adequate disclosure of the structure of a firewall is disclosed in the ‘564 patent’s specification. The software on the firewall or router for performing the functions is explained through the algorithms disclosed in Figure 1 which illustrates a packet transmission control system 10 for managing traffic 14 between at least two data networks 18, 22. The firewall 42 includes hardware and software providing a non-redundant connection 46 between the networks 18, 22 and serves to control packet transmission between the networks 18, 22. The algorithm discloses maximum transmission rates (one of 12, 9, 20, or 4) and an associated class of data packet 66.[65]

Figure 1 discloses an algorithm and diagram by flowchart for classifying data packets 38 received at the firewall 42 related to the consumption of at least one resource. The flowchart further shows associating a maximum acceptable transmission rate 62 with each class 66 of data packet 38 received at the firewall 42. The flowchart further shows the maximum transmission rate can be set as a limit on the transmission rate of packets across the firewall. When transmission rates 62 from the firewall 42 are so limited, packet flooding and other over usage type distributed denial of service attacks cannot be effectively launched through the network connection.[66] Moreover, a firewall inherently possesses the capability to inspect and label or mark (i.e., classify) data packets based on their properties.[67] This would include available location information that accurately and reliably provides the firewall with the locations through which attackers are sending flood attacks[68] as would be understood by one of ordinary skill in the art and as is disclosed in the highly related ‘497 patent.[69] The patents cited in the prior art of this specification, US6154775 and US6304975, both show that firewalls are well-known in the prior art to have the

[65] *See* Doc. No. 1-2 at Figure 1.
[66] *See* Doc. No. 1-2 at 5:10-31.
[67] *See* Narayanaswamy Decl. at ¶s 28-29.
[68] A flood attach is commonly known as Distributed Denial of Service (“DDoS”).
[69] *See* Doc. No. 1-3 at 3:64-66 (“which is done via packet marks provided by router....).

ability to inspect and classify packets by their properties. In this invention, such classification would also include inspecting the data packets to discern the location information added to those packets by cooperating routers as disclosed in the highly relevant '497 patent. Using data packets that incorporate marks encoding the locations taken by the packet through a cooperating network of routers was not known in the art.[70]

Lastly, it is common parlance for one of ordinary skill in the art to use a firewall for limiting the transmission rate from the firewall to the maximum acceptable transmission rate for a class of data packet. The patents cited in the prior art of this specification, US6154775 and US6304975, both show that firewalls are well-known in the prior art to have the ability to inspect and classify packets by their properties. In this invention, such classification would also include inspecting the data packets to discern the path information added to those packets by cooperating routers as disclosed in the highly relevant '497 patent. Using data packets that incorporate marks encoding the paths taken by the packet through a cooperating network of routers was not known in the art.[71]

9. means for said firewall to measure the amount of service requested by each packet[72]

Plaintiff's proposed construction	**Defendant's proposed construction**	**By:**
Function: measuring the amount of service requested by each packet Structure: 3:20 - 3:24; 4:17 - 4:23; 4:61 - 4:64; 5:62 - 5:64; Figure 4	Indefinite	J

The flow chart and algorithm for this claim term is disclosed in Figure 4. A firewall 42 further identifies data packets 38 as requests for services 98 of at least one type requiring transmission of data packets 38 from locations 78 within one of the networks 18 to another of the networks 22. The firewall 42 measures the amount of service 36 requested by each identified

[70] *See* Narayanaswamy Decl. at ¶29.
[71] *See* id. at ¶31.
[72] Claim 4 of the '564 patent.

packet 38. Based upon this identification and this measure of amount of service 36, firewall 42 will thus limit the transmission rate for data packets 38 that are requests for services 98 based upon the type of service 98 requested in order to limit usage of each Service 98.[73] Two exemplary services disclosed are "requests for file transfer to B" and "requests for web page retrieval from C."[74] The disclosure of this algorithm is sufficient for structure for one of ordinary skill in the art to practice the invention.[75]

10. whereby, packet flooding and other over usage type distributed denial of service attacks cannot be effectively launched through said non-redundant connection[76]

Plaintiff's proposed construction	Defendant's proposed construction	By:
No construction necessary	Indefinite	D

Construction of long claim terms is disfavored.[77] Additionally, this "whereby" clause does not provide a limitation on the claim and need not be construed.[78] If a whereby clause adds nothing to the claims and simply characterizes the intended result of the executing steps, it need not be construed by the court.[79] Here, no meaningful limitation is added by this "whereby" clause and no construction is necessary.

11. whereby, said firewall will limit the transmission rate for data packets of each class from locations within one of said networks to provide proportionally fair forwarding service to other locations within said network that communicates

[73] *See* Doc. No. 1-2 at 5:52-64.
[74] *See* Doc. No. 1-2 at Figure 4 (also shown in Figures 5 and 6).
[75] *See* Narayanaswamy Decl. at ¶33.
[76] Claim 1 of the '564 patent
[77] *Ihance, Inc. v. Eloqua Ltd.*, Civ. Act. No. 2:11cv2572012, U.S. Dist. LEXIS 62514, at *15, *16 (E.D. Va. May 2, 2012) (describing a 42-word term as "lengthy" and declining to construe the term); *Honeywell Int'l, Inc. v. Nikon Corp.*, 589 F. Supp. 2d 433, 440–444 (D. Del. 2008) (describing a 24-word term as "rather lengthy," then focusing on 2 words of the claim term, and ultimately declining to construe the 24-word term).
[78] *Tex. Instruments Inc. v. U.S. Int'l Trade Comm'n*, 988 F.2d 1165, 1172 (Fed.Cir.1993) (concluding, in process claims, that the whereby clauses described "the result of arranging the components of the claims in the manner recited in the claims" and thus were not limitations).
[79] *See Minton*, 336 F.3d at 1381.

through said non-redundant connection[80]

Plaintiff's proposed construction	Defendant's proposed construction	By:
No construction necessary	Indefinite	D

Construction of long claim terms is disfavored.[81] Additionally, this "whereby" clause does not provide a limitation on the claim and need not be construed.[82] "If a whereby clause adds nothing to the claims and simply characterizes the intended result of the executing steps, it need not be construed by the court.[83] Here, no meaningful limitation is added by this "whereby" clause and no construction is necessary.

12. means for said firewall to measure the amount of service consumed in order to send each identified response data packet[84]

Plaintiff's proposed construction	Defendant's proposed construction	By:
Function: measuring, for the firewall, the amount of service of each type consumed to send each identified response data packet Structure: 3:24 - 3:27; 4:23 - 4:31; 4:65 - 5:03; 5:65 - 6:13; Figure 5	Indefinite	J

Figure 5 discloses flowchart and algorithm for a firewall for classifying data packets 38 received at the firewall 42 wherein the firewall further includes identifying data packets 38 as requests for services 98 of at least one type requiring transmission of data packets 38 from locations

[80] Claim 2 of the '564 patent
[81] *Ihance, Inc. v. Eloqua Ltd.*, Civ. Act. No. 2:11cv2572012, U.S. Dist. LEXIS 62514, at *15, *16 (E.D. Va. May 2, 2012) (describing a 42-word term as "lengthy" and declining to construe the term); *Honeywell Int'l, Inc. v. Nikon Corp.*, 589 F. Supp. 2d 433, 440–444 (D. Del. 2008) (describing a 24-word term as "rather lengthy," then focusing on 2 words of the claim term, and ultimately declining to construe the 24-word term).
[82] *Tex. Instruments Inc. v. U.S. Int'l Trade Comm'n*, 988 F.2d 1165, 1172 (Fed.Cir.1993) (concluding, in process claims, that the whereby clauses described "the result of arranging the components of the claims in the manner recited in the claims" and thus were not limitations).
[83] *See Minton*, 336 F.3d at 1381.
[84] Claim 5 of the '564 patent

78 within one of the networks 18 to another of the networks 22 and identifying data packets 38 as responses to earlier service requests 98 of at least one type from a location 78 within one of the networks 18 requiring transmission of data packets 38 to another of the networks 22. Firewall 42 measures the amount of service 36 requested by each identified data packet 38. Based upon this identification and this measure of amount of service 36, the firewall 42 will thus limit the transmission rate for data packets 38 that are requests for services 98 based upon the type of service 98 requested in order to limit usage of each service 98.[85]

13. means for storing and recalling past measurements of amounts of service provided for each type of service[86]

Plaintiff's proposed construction	**Defendant's proposed construction**	**By:**
Function: storing and recalling past measurements of amounts of service provided for each type of service Structure: 3:24 - 3:29; 4:32 - 4:39; 5:03 - 5:05; 6:14 - 6:20; Figure 6	Indefinite	J

This is not a term subject to a 112(f) analysis. The claim term is for computer memory for storing and recalling data.[87] Computer memory is a well-known example of a term not subject to 112(f).[88] As an alternate position, Plaintiff identifies structure from the patent.

14. whereby, said firewall will limit the transmission rate for data packets that are requests for each type of service to limit usage of each service over extended periods of time [89]

Plaintiff's proposed construction	**Defendant's proposed construction**	**By:**

[85] *See* Doc. No. 1-2 at 5:65-6:13; *See* Narayanaswamy Decl. at ¶35.
[86] Claim 6 of the '564 patent
[87] *See* Narayanaswamy Decl. at ¶37.
[88] *TecSec, Inc.* 731 F.3d at 1437 (A "system memory" is sufficient structure to perform the "storing data" function. To those skilled in the art, a system memory is a specific structure that stores data.).
[89] Claim 6 of the '564 patent

No construction necessary	Indefinite	D

Construction of long claim terms is disfavored.[90] Additionally, this "whereby" clause does not provide a limitation on the claim and need not be construed.[91] If a whereby clause adds nothing to the claims and simply characterizes the intended result of the executing steps, it need not be construed by the court.[92] Here, no meaningful limitation is added by this "whereby" clause and no construction is necessary.

15. means for classifying data packets received at a/said host computer/router into wanted data packets and unwanted data packets/...by path[93]

Plaintiff's proposed construction	**Defendant's proposed construction**	**By:**
Function: classifying data packets received at a host computer into wanted data packets and unwanted data packets/...by path Structure: 3:30 - 3:42; 5:29 - 5:33; 6:12 - 6:25; Figure 1; Figure 4; Figure 7	Indefinite	J

16. means for associating a maximum acceptable processing rate with each class of data packet received at said computer[94]

Plaintiff's proposed construction	**Defendant's proposed construction**	**By:**
Function: associating a maximum acceptable processing rate with each class of data packet received at said computer Structure: 3:43 - 3:61; 5:33 - 5:39; 6:26 - 6:46; Figure 2; Figure 5; Figure 8	Indefinite	J

[90] *Ihance, Inc. v. Eloqua Ltd.*, Civ. Act. No. 2:11cv2572012, U.S. Dist. LEXIS 62514, at *15, *16 (E.D. Va. May 2, 2012) (describing a 42-word term as "lengthy" and declining to construe the term); *Honeywell Int'l, Inc. v. Nikon Corp.*, 589 F. Supp. 2d 433, 440–444 (D. Del. 2008) (describing a 24-word term as "rather lengthy," then focusing on 2 words of the claim term, and ultimately declining to construe the 24-word term).

[91] *Tex. Instruments Inc. v. U.S. Int'l Trade Comm'n*, 988 F.2d 1165, 1172 (Fed.Cir.1993) (concluding, in process claims, that the whereby clauses described "the result of arranging the components of the claims in the manner recited in the claims" and thus were not limitations).

[92] *See Minton*, 336 F.3d at 1381.

[93] Claims 1, 4, 13 and 16 of the '497 patent.

[94] Claim 1 of the '497 patent.

Plaintiff groups these two terms together as the disclosure of structure and argument is largely coextensive. However, while Plaintiff contends these terms do not require the 112(f) analysis, Plaintiff's identified function and structure are provided in the boxed chart with argument and explanation following.

These claim terms are not subject to the requirements of 112(f) because from the perspective of one of ordinary skill in the art, the preamble of claim 1 of the '497 patent,[95] followed by the subsequent claim language provide the structure of a router or firewall for each of "means for classifying..." and "means for associating..."[96] Both a router and a firewall have a very well-defined meaning in the art. A firewall is a device which is placed between two networks by the owner of one of those networks to safeguard that network from various network attacks. These capabilities include identifying sets of data packets by certain properties (referred to as classification) and allocating a processing rate to those packets identified by class. In the current invention, this method is extended to include information about the path taken by the packets as they traverse the computer network before they arrive at the firewall. A router is a device which forwards data packets to locations within a computer network. The data packets are forwarded along communication lines or paths between the appropriate parts of the computer network. It is very common for a router and/or a firewall to be part of securing a computer network for inspecting the contents of packets, and/or limiting the rates of transmission of specific sets of packets identified by properties (i.e., classification) including blocking that set of packets entirely.[97]

One of ordinary skill in the art would understand that a router or a firewall provides the following capabilities:

[95] *See* Doc. No. 1-3 at 8:9-27.
[96] *See* Narayanaswamy Decl. at ¶40.
[97] *See* id. at ¶40.

1. classifying data packets received at a host computer and

2. associating a maximum acceptable processing rate...

based on the literal language of the claim and the specification.[98] First, the claim sets forth in the preamble that a packet flooding defense system of the invention includes a router.[99] Second, in common parlance to one of ordinary skill in the art, an as provided in the specification, the "at least one firewall" comprises "hardware and software serving to control packet transmission"[100] which one of ordinary skill in the art would know is a firewall that can be configured by software to provide the capabilities described.[101] Thus, it is my opinion that sufficient structure is provided in the claim that each of "means for classifying..." and means for associating..." are not properly considered as means plus function claim terms as one of ordinary skill in the art would appreciate the structure disclosed is a router or a firewall. However, adequate disclosure of the structure of a router and a firewall is also disclosed in the specification.

The claimed invention describes how the forwarding path for each packet is associated with that packet, thereby making it possible for a receiving computer to know that information. The software, or configuration, at the firewall is explained through the algorithms disclosed in Figure 1 by flowchart and diagram where a Class A and Class B (38) of a maximum acceptable processing rate (34) are assigned by the firewall to each data packet (30). The description provides that the computer can use the information, the maximum acceptable processing rate, to allocate the processing rate for each class (38) in a desired way among the places from which packets (30)

[98] *See* Narayanaswamy Decl. at ¶s40-41.
[99] *See* Doc. No. 1-3 at 8:9-11.
[100] *See* Doc. No. 1-3 at 4:47-60.
[101] *See* Narayanaswamy Decl. at ¶s40-41.

are transmitted.[102] Figure 2, Figure 3, Figure 4, Figure 5, and Figure 6 illustrate additional embodiments, or algorithms, in which path information associated with each packet can be combined with other properties to classify the packet and assign it a transmission rate.[103] Figure 7, Figure 8 and Figure 9 illustrate how a firewall protecting a network communicates the rate limit for packets routed to it or routed to it by class functions.[104] Moreover, the marking of data packets by a firewall or router is within the ordinary parlance of one of ordinary skill in the art and as is disclosed in the '497 patent.[105] Prior art discussed in the specification of the '497 patent (US5455865 and US6044402 for example) rely on the well-understood and accepted functionality of routers to maintain flow information between source and destination addresses.[106] Marking of data packets that traverse a router is well-known in the art. Marking of data packets to encode path information is unique to this invention, and anyone familiar with firewalls would understand how to use a firewall capability to encode paths. The specification describes how a firewall and a router can add to packet information about the interface points where the packet entered the firewall or router. Anyone familiar with firewalls or routers would be able to implement this in different ways. Using data packet marks that encode the forwarding path of the path in a cooperating network of routers was not known in the prior art. The importance of the path information is that it is generated by routers in the network, and, therefore, not something that the attacker controls. The packet path information is very reliable and accurate in identifying the directions from which attackers are mounting attacks.[107]

---

[102] *See* Narayanaswamy Decl. at ¶42.
[103] *See* Doc. No. 1-3 at Figures 2, 3, 4, 5, and 6; *See* Narayanaswamy Decl. at ¶42.
[104] *See* Doc. No. 1-3 at Figures 7, 8, and 9; *See* Narayanaswamy Decl. at ¶42.
[105] *See* Doc. No. 1-3 at 3:64-66 ("which is done via packet marks provided by router...."); *See* Narayanaswamy Decl. at ¶42.
[106] *See* Narayanaswamy Decl. at ¶41.
[107] *See* id. at ¶42.

The ‘497 patent described the shortcomings of the prior art at 2:23-29 wherein it provided an issue is the lack of a reliable way to associate incoming packets with those users among whom bandwidth should be fairly allocated. The other is lack of control over what packets arrive. The solution described here to both of these problems requires help from the routers that forward packets to the victim.

The ‘497 patent provides several technological solutions on overcoming these prior art issues. At 3:62-4:5, the ‘497 patent teaches:

> ... a path (which is not controlled by the attacker) is used to determine the actual direction of the packet flow towards the victim. Bandwidth is allocated based upon path (which is done via packet marks provided by routers leading up to the victim). In other words this invention uses attacker-independent information about the path a packet takes to allocate forwarding bandwidth in a router. The part that makes this invention completely different from Chang, et al, is that the information has to be attacker-independent (i.e., sender-independent) in order to work as a defense.

Further, at 8:18-24, the ‘497 patent teaches that a host computer is able to identify the path by the packet mark applied at a router:

> means for said computer to find information for packets it receives regarding the path by which said packets came to said computer via packet marks provided by routers leading to said host computer; said path comprising all routers in said network via which said packets are routed to said computer; and

Further, at 9:01-04, the ‘497 patent teaches a router is able to identify the path of a packet by packet mark provided by a router:

> means for said router to find information for packets it receives regarding the path by which said packets came to said router via packet marks provided by routers leading to said host computer;

Further, at 9:49-9:53, the ‘497 patent teaches a host computer is able to determine a path by which data packets arrive at a host computer by packet marks:

> determining a path by which data packets arrive at a host computer via packet marks provided by routers leading to said host computer; said path comprising all routers in said network via which said packets are routed to said computer;

Further, at 10:29-34, the '497 patent teaches a downstream router is able to determine a path by packet marks from an upstream router:

> determining a path by which data packets arrive at said router via packet marks provided by routers leading to said host computer; said path comprising all routers in said network via which said packets are routed to said computer;

Further, at 11:10-16, the '497 patent teaches a system of cooperating routers wherein a host computer is able to identify the path a packet comes in on by packet marks:

> means for determining a path by which data packets arrive at a host computer via packet marks provided by routers leading to said host computer; said path comprising all routers in said network via which said packets are routed to said computer;

Further, at 12:06-10, the '497 patent teaches a system of cooperating routers wherein a router is able to identify the path a packet comes in on by packet marks:

> means for a router to determine a path by which said packets came to said router via packet marks provided by routers leading to said router; said path comprising all routers in said network via which said packets are routed to said computer;

Figures 1, 2, 3, 4, 5, and 6 each illustrate illustrative methods of determining, by packet marking, how the path a packet takes is identified. These Figures, in cooperation with the written description, further provide various algorithms, by flowchart, used by the claimed invention to perform the claimed functions.[108]

Lastly, it is common parlance for one of ordinary skill in the art to use a router or a firewall to (1) mark data packets and for (2) associating a maximum acceptable processing rate with each

[108] *See* Narayanaswamy Decl. at ¶51.

class of data packet. Prior art cited in this patent specification including US5455865 and US 5353353 use similar capabilities to implement other network attack defenses. In this patent specification the same capabilities are utilized to limit the rate of packets with added path information.[109] The '497 patent's specification describes how processing rate limits can be used to allocate the processing rates available for packets of each class in a desired manner.[110]

17. means for said computer to find information for packets it receives regarding the path by which said packets came to said computer via packet marks provided by routers leading to said host computer[111]

Plaintiff's proposed construction	Defendant's proposed construction	By:
Function: finding information, for said computer, for packets received regarding the path by which said packets came to said computer via packet marks provided by routers leading to said host computer Structure: 3:62 - 4:20; 5:40 - 5:44; 6:46 - 6:51; Figure 3; Figure 6; Figure 9	Indefinite	J

18. means in said computer for using said information to allocate the processing rate available for unwanted data packets to be less than or equal to said maximum acceptable processing rate[112]

Plaintiff's proposed construction	Defendant's proposed construction	By:
Function: allocating the processing rate available for unwanted data packets to be less than or equal to said maximum acceptable processing rate Structure: 3:30 - 3:42; 5:29 - 5:33; 6:12 - 6:25; Figure 1; Figure 4; Figure 7	Indefinite	J

[109] *See* Narayanaswamy Decl. at ¶s 53, 55.
[110] *See* Doc. No. 1-3 at 3:30-42.
[111] Claim 1 of the '497 patent.
[112] Claim 1 of the '497 patent.

Plaintiff groups these two terms together as the disclosure of structure and argument is largely coextensive. Plaintiff's identified function and structure are provided in the boxed chart with argument and explanation following.

The means for the computer (1) to find information for packets it receives and (2) to use the information to allocate processing rate available for unwanted data packets to be less than or equal to said maximum acceptable processing rate, is disclosed in the algorithm shown in Figure 1. The software, or configuration, at the computer is explained through the algorithms disclosed in Figure 1 by flowchart and diagram where a Class A and Class B (38) of a maximum acceptable processing rate (34) are assigned by the firewall to each data packet (30). The description provides that the computer can use the information, the maximum acceptable processing rate, to allocate the processing rate for each class (38) in a desired way among the places from which packets (30) are transmitted.[113] Figure 2, Figure 3, Figure 4, Figure 5, and Figure 6 illustrate additional embodiments, or algorithms, in which path information associated with each packet can be combined with other properties to classify the packet and assign it a processing rate.[114] Figure 7, Figure 8 and Figure 9 illustrate how a firewall protecting a network communicates the rate limit for packets routed to it or routed to it by class functions.[115]

19. means for said router to find information for packets it receives regarding the path by which said packets came to said router via packet marks provided by routers leading to said host computer[116]

Plaintiff's proposed construction	**Defendant's proposed construction**	**By:**
Function: finding information for packets received at the router	Indefinite	J

[113] *See* Narayanaswamy Decl. at ¶57.
[114] *See* Doc. No. 1-3 at Figures 2, 3, 4, 5, and 6.
[115] *See* Doc. No. 1-3 at Figures 7, 8, and 9.
[116] Claim 4 of the '497 patent.

regarding the path by which said packets came to said router via packet marks provided by routers leading to said host computer Structure: 3:62 - 4:20; 5:40 - 5:44; 6:46 - 6:51; Figure 3; Figure 6; Figure 9		

20. means in said router for said router to use said information to allocate the transmission rate for unwanted data packets to be less than equal to said maximum acceptable transmission rate[117]

Plaintiff's proposed construction	**Defendant's proposed construction**	**By:**
Function: allocating the transmission rate for unwanted data packets to be less than equal to said maximum acceptable transmission rate Structure: 3:62 - 4:20; 5:40 - 5:44; 6:46 - 6:51; Figure 3; Figure 6; Figure 9	Indefinite	J

21. means for determining a path by which data packets arrive at a host computer via packet marks provided by routers leading to said host computer[118]

Plaintiff's proposed construction	**Defendant's proposed construction**	**By:**
Function: determining a path by which data packets arrive at a host computer via packet marks provided by routers leading to said host computer Structure: 3:30 - 3:42; 5:29 - 5:33; 6:12 - 6:25; Figure 1; Figure 4; Figure 7	Indefinite	J

22. means for assigning a maximum acceptable processing rate to each class of data packet[119]

Plaintiff's proposed construction	**Defendant's proposed construction**	**By:**
Function: assigning a maximum acceptable processing rate to each class of data packet Structure: 3:30 - 3:42; 5:29 - 5:33; 6:12 - 6:25; Figure 1;	Indefinite	J

[117] Claim 4 of the '497 patent.
[118] Claim 13 of the '497 patent.
[119] Claim 13 of the '497 patent.

Figure 4; Figure 7		

23. means for allocating a processing rate equal to or less than said maximum acceptable processing rate to said unwanted data packets[120]

Plaintiff's proposed construction	**Defendant's proposed construction**	**By:**
Function: allocating a processing rate that is equal to or less than said maximum acceptable processing rate to said unwanted data packets Structure: 3:30 - 3:42; 5:29 - 5:33; 6:12 - 6:25; Figure 1; Figure 4; Figure 7	Indefinite	J

Plaintiff groups these five terms together as the disclosure of structure and argument is largely coextensive. However, while Plaintiff contends these terms do not require the 112(f) analysis, Plaintiff's identified function and structure are provided in the boxed chart with argument and explanation following.

The means (1) for the router to find information for packets it receives regarding the path ...; (2) in the router for the router to use the information...; (3) determining a path by which data packets arrive at a host computer...; (4) assigning a maximum acceptable processing rate...; and, (5) allocating a processing rate..., are disclosed in the algorithm shown in Figure 3. However, the structure of a router is provided in the claim language and this term is not subject to 112(f). It is common parlance to one of ordinary skill in the art for a router or firewall to perform each of these functions.[121]

Additionally, the software, or configuration, at the router is explained through the algorithms disclosed in Figure 3 by flowchart and diagram where a Class A and Class B (38) of a

[120] Claim 13 of the '497 patent.
[121] *See* Narayanaswamy Decl. at ¶s 61-62, 64-65, 67-68, 70-71, 73-74.

maximum acceptable processing rate (34) are assigned by the firewall to each data packet (30). The description provides that the computer can use the information, the maximum acceptable processing rate, to allocate the processing rate for each class (38) in a desired way among the places from which packets (30) are transmitted.[122] A router 22 is capable of receiving information regarding maximum acceptable transmission rate 70 for each class 38 of data packet 30 being transmitted to the computer 18 and the router 22 is capable of controlling the rate of transmission of each class 38 of data packets 30 to the computer 18.[123] Figure 2, Figure 1, Figure 4, Figure 5, and Figure 6 illustrate additional embodiments, or algorithms, in which path information associated with each packet can be combined with other properties to classify the packet and assign it a processing rate.[124] Figure 7, Figure 8 and Figure 9 illustrate how a firewall protecting a network communicates the rate limit for packets routed to it or routed to it by class functions.[125]

Lastly, it is common parlance for one of ordinary skill in the art to use a router or a firewall to (1) for the router to find information for packets it receives regarding the path ...; (2) in the router for the router to use the information...; (3) determining a path by which data packets arrive at a host computer...; (4) assigning a maximum acceptable processing rate...; and, (5) allocating a processing rate.... Prior art cited in this patent specification including US5455865 and US 5353353 use similar capabilities to implement other network attack defenses. In this patent specification the same capabilities are utilized to limit the rate of packets with added path information.[126] The '497

[122] *See* id.
[123] *See* Doc. No. 1-3 at 6:46-51.
[124] *See* Doc. No. 1-3 at Figures 2, 3, 4, 5, and 6.
[125] *See* Doc. No. 1-3 at Figures 7, 8, and 9.
[126] *See* Narayanaswamy Decl. at ¶s 53, 55.

patent's specification describes how processing rate limits can be used to allocate the processing rates available for packets of each class in a desired manner.[127]

IV. CONCLUSION

Plaintiff respectfully requests the Court adopt its constructions.

Respectfully submitted,

Ramey & Schwaller, LLP

William P. Ramey, III
Texas Bar No. 24027643
wramey@rameyfirm.com
5020 Montrose Blvd., Ste. 800
Houston, Texas 77006
(713)426-3923
(832)900-4941 (fax)

Attorneys for PacSec3, LLC

CERTIFICATE OF SERVICE

The undersigned certifies that the foregoing document was filed electronically in compliance with local rules and the rules of civil procedure. As such, this pleading was served on all counsel who have consented to electronic service on April 12, 2021.

William P. Ramey, III
William P. Ramey, III

[127] *See* Doc. No. 1-3 at 3:30-42.